(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10312459 A**

(43) Date of publication of application: **24 . 11 . 98**

(51) Int. Cl **G06T 7/00**

(21) Application number: **10060815**

(22) Date of filing: **12 . 03 . 98**

(30) Priority: **13 . 03 . 97 JP 09 58795**

(71) Applicant: **HITACHI LTD**

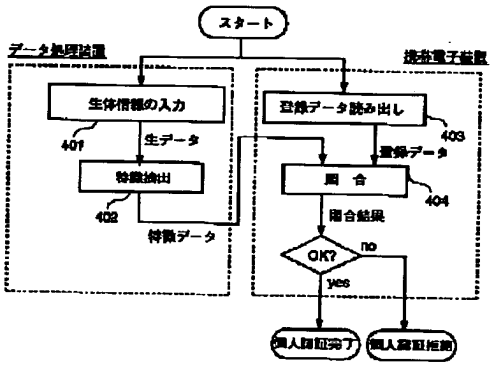
(72) Inventor: **OKI MASARU**
SAKAGUCHI TAKAHIRO
SATOU KAZUYASU

(54) PORTABLE ELECTRONIC DEVICE AND PERSONAL AUTHENTICATION METHOD IN WHICH BIOLOGICAL INFORMATION IS USED

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a personal authentication method with high security by using biological information which is impossible to be stolen or imitated.

SOLUTION: Characteristic volume of the biological information is stored as registration data in a portable electronic device (IC card). A user inputs one's biological information in a data processor (IC card terminal, etc.) (401). The characteristic volume is extracted regarding the inputted biological information (402) and transmitted to the portable electronic device by the data processor. The personal authentication is performed by collating characteristic data inputted from the data processor with the registration data in the portable electronic device.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－312459

(43)公開日　平成10年(1998)11月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０

審査請求　未請求　請求項の数24　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－60815

(22)出願日　平成10年(1998)３月12日

(31)優先権主張番号　特願平9－58795

(32)優先日　平９(1997)３月13日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大木　啓
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　坂口　隆宏
東京都国分寺市東恋ケ窪三丁目１番地１
日立超エル・エス・アイ・エンジニアリング株式会社内

(72)発明者　佐藤　和恭
茨城県土浦市神立町502番地　株式会社日立製作所機械研究所内

(74)代理人　弁理士　小川　勝男

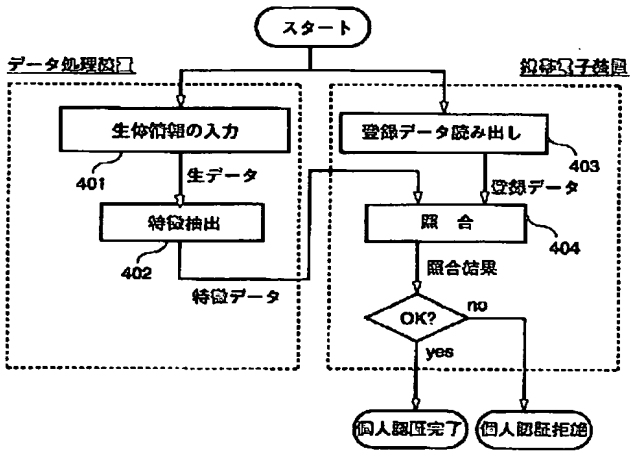
(54)【発明の名称】　携帯電子装置及び生体情報を用いた個人認証方法

(57)【要約】

【課題】　盗難や模倣が不可能な生体情報を用いて、セキュリティの高い個人認証方法を提供する。

【解決手段】　携帯電子装置（ＩＣカード）には生体情報の特徴量を登録データとして格納しておく。使用者は、自分の生体情報をデータ処理装置（ＩＣカードターミナル等）に入力する(401)と、データ処理装置は、入力された生体情報について特徴量を抽出して(402)、携帯電子装置に送信する。携帯電子装置ではデータ処理装置より入力された特徴データと登録データとを照合する(404)ことにより個人認証を行う。

図４



1

【特許請求の範囲】

【請求項１】第一の生体情報の特徴量を登録データとして記憶するメモリと、データ処理装置から認証の対象となる第二の生体情報の特徴量を特徴データとして受信する送受信インタフェースと、上記登録データと上記特徴データとを比較照合するプロセッサとを有することを特徴とする携帯電子装置。

【請求項２】請求項１記載の携帯電子装置において、

上記携帯電子装置は耐タンパー性装置であることを特徴とする携帯電子装置。

【請求項３】請求項１記載の携帯電子装置において、

上記生体情報は、指紋、網膜パターン、音声、筆跡のいずれかであることを特徴とする携帯電子装置。

【請求項４】第一の生体情報の特徴量を登録データとして保持する携帯電子装置の個人認証を行うデータ処理装置において、

デジタル信号に変換された第二の生体情報を生データとして受信する第一の送受信インタフェースと、上記生データから特徴量を抽出するプロセッサと、上記抽出された特徴量を上記第二の生体情報の特徴データとして上記携帯電子装置に送信する第二の送受信インタフェースとを有することを特徴とするデータ処理装置。

【請求項５】第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を抽出し、上記抽出した特徴量を特徴データとして上記携帯電子装置に送信し、

上記携帯電子装置は、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項６】第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データを上記部分登録データにより正規化し、上記正規化された特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記正規化された特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項７】請求項６記載の個人認証方法において、

上記データ処理装置は、上記特徴データから上記部分登録データにより、上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記正規化された特徴データとして上記切り出された特徴データを上記携帯電子装置に送信することを特徴とする個人認証方法。

2

【請求項８】第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記位置合わせについての情報に基づき、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項９】請求項８記載の個人認証方法において、

上記データ処理装置は、上記位置合わせにより、上記特徴データから上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記切り出された特徴データを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項１０】請求項８記載の個人認証方法において、

上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記特徴データと上記登録データのうち上記部分登録データを除いた部分とにより第二の照合処理を行うことを特徴とする個人認証方法。

【請求項１１】請求項１０記載の個人認証方法において、

上記照合処理は、上記登録データA_i（$1 \leqq i \leqq n$）のいずれかと上記特徴データX_j（$1 \leqq j \leqq m$）のいずれかとの組合せの距離d_{ij}（$1 \leqq i \leqq n$，$1 \leqq j \leqq m$）の累積距離Ｄの最小値と所定の閾値との比較により行い、

上記第一の照合処理において計算対象とする上記部分登録データA_i（$1 \leqq i \leqq u$）と上記特徴データX_jとの組合せの範囲は、上記第二の照合処理において計算対象とする上記登録データのうち上記部分登録データを除いた部分A_i（$u+1 \leqq i \leqq n$）と上記特徴データX_jとの組合せの範囲よりも広く設定されていることを特徴とする個人認証方法。

【請求項１２】請求項１０記載の個人認証方法において、

上記生体情報は、音声または筆跡であることを特徴とする個人認証方法。

【請求項１３】第一の生体情報の特徴量を登録データと

して保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データについて所定の複数の近傍との距離を算出し、上記特徴データと上記算出された距離とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記登録データと一致する上記複数の近傍のいずれかを選択し、上記選択された近傍と上記特徴データとの距離を用いることにより、上記特徴データと上記登録データとを照合することを特徴とする個人認証方法。

【請求項１４】請求項１３記載の個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項１５】請求項１４記載の個人認証方法において、

上記データ処理装置は、上記位置合わせについての情報に基づき、上記携帯電子装置に保持された登録データに相当する部分の特徴データについて所定の複数の近傍との距離を算出し、上記特徴データと上記算出された距離とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項１６】請求項１４記載の個人認証方法において、

上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記登録データのうち上記部分登録データを除いた部分について、上記登録データの部分と一致する上記複数の近傍のいずれかを選択し、上記選択された近傍と上記特徴データとの距離を用いることにより、第二の照合処理を行うことを特徴とする個人認証方法。

【請求項１７】第一の生体情報の特徴量を登録データとして保持する携帯電子装置とデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記データ処理装置は、入力された第二の生体情報から特徴量を特徴データとして抽出し、上記特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記特徴データと上記登録データの差データを算出し、上記算出した差データを暗号化処理して上記データ処理装置に送信し、

上記データ処理装置は、上記暗号化された差データに基づき上記特徴データと上記登録データとについて前照合を行い、上記前照合結果を上記携帯電子装置に送信し、

上記携帯電子装置は、上記前照合結果を復号し、後照合を行うことを特徴とする個人認証方法。

【請求項１８】請求項１７記載の個人認証方法において、

上記携帯電子装置は発生させた乱数により、上記差データをスクランブルして上記データ処理装置に送信し、上記乱数により上記データ処理装置より送信された上記前照合結果を復号することを特徴とする個人認証方法。

【請求項１９】請求項１７記載の個人認証方法において、

上記携帯電子装置は、上記登録データの一部分を切り出し、上記切り出された部分登録データを上記データ処理装置に送信し、

上記データ処理装置は、上記特徴データと上記部分登録データとにより、上記特徴データと上記携帯電子装置に保持された登録データとの位置合わせを行い、上記特徴データと上記位置合わせについての情報とを上記携帯電子装置に送信することを特徴とする個人認証方法。

【請求項２０】請求項１９記載の個人認証方法において、

上記データ処理装置は、上記位置合わせにより、上記特徴データから上記携帯電子装置に保持された上記登録データに相当する部分を切り出し、上記切り出された特徴データを上記携帯電子装置に送信し、

上記携帯電子装置は、上記切り出された特徴データと上記登録データの差データを算出することを特徴とする個人認証方法。

【請求項２１】請求項１９記載の個人認証方法において、

上記データ処理装置は、上記特徴データと上記部分登録データとにより第一の照合処理を行い、上記特徴データと上記第一の照合処理結果とを上記携帯電子装置に送信し、

上記携帯電子装置は、上記第一の照合処理結果に基づき、上記登録データのうち上記部分登録データを除いた部分と上記特徴データとの差データを算出し、上記算出した差データを暗号化処理して上記データ処理装置に送信し、

上記データ処理装置は、上記暗号化された差データに基づき上記特徴データと上記登録データとについて第二の照合処理における前照合を行い、上記前照合結果を上記携帯電子装置に送信し、

上記携帯電子装置は、上記前照合結果を復号し、第二の照合処理における後照合を行うことを特徴とする個人認

証方法。

【請求項２２】第一の生体情報の特徴量を登録データとして保持する携帯電子装置と外部情報処理装置とネットワークにより接続されたデータ処理装置とにより、上記携帯電子装置の個人認証を行う個人認証方法において、

上記携帯電子装置は、上記データ処理装置より第二の生体情報の特徴量を特徴データとして入力を受け、上記登録データと上記特徴データとを照合し、上記照合の結果に基づき、個人認証の成否を判断し、

上記個人認証が成功した場合には、上記携帯電子装置は上記外部情報処理装置から暗号化されて送信される第一の情報を受信し、

上記携帯電子装置は、上記受信した第一の情報に所定の処理に必要な第二の情報を付加して暗号化し、上記外部情報処理装置に送信することを特徴とする個人認証方法。

【請求項２３】請求項２２記載の個人認証方法において、

上記外部処理装置は、上記携帯電子装置から送信された情報を復号し、上記第一の情報が、上記外部処理装置が上記携帯電子装置に送信した第一の情報と一致していることを条件に、上記所定の処理を実行することを特徴とする個人認証方法。

【請求項２４】請求項２２記載の個人認証方法において、

上記外部処理装置は、上記第一の情報として現在時刻を送信することを特徴とする個人認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカード等を代表とする携帯電子装置の個人認証やインターネットなどのネットワークを通じた個人認証や電子署名に関する。例えば、第三者が不正に使用することが出来ない安全な電子通貨や、キャッシュレスショッピング、オンラインショッピング、ホームバンキング等の電子商取引に利用できる。

【０００２】

【従来の技術】現在、銀行の預金引き下ろしや商品の購入において特定の個人を認証するため、情報を記憶する磁気ストライプを有するカード（以下、磁気カードと呼ぶ）が広く用いられている。キャッシュカードにより銀行の自動預け払い機から現金を引き出す場合には、暗証番号により個人認証を行う。クレジットカードにより商品購入する場合には、クレジットカード裏面の署名と商品購入時の署名とを照合し、個人認証を行っている。

【０００３】このような個人認証方法には、セキュリティに関する問題点が指摘されている。キャッシュカードとその暗証番号とが第三者に盗まれた場合、容易に第三者によって預金が引き出されてしまう。クレジットカードは、第三者が署名を真似ることで盗用されることもある。

【０００４】そこで、磁気カードに代えてＩＣカードを使用することにより、カードに格納できる情報量を増大できることに着目し、指紋や網膜パターンあるいは音声等の生体情報を使用して個人認証する方法が提案されている。これら提案の多くは、生体情報を利用する個人認証には相当の処理負荷を要するため、ＩＣカードターミナルで処理することが想定されている。しかし、かかる処理もまた、個人登録データが外部に流出すること、ＩＣカードターミナルに対しては比較的容易に認証プログラムの第三者の改変が可能であることにより、セキュリティ上の問題がある。

【０００５】そこで、特開昭６１－１９９１６２号公報「個人識別システム」には、暗証コードとして指紋を用い、指紋の特徴抽出及び照合処理をＩＣカードで行うアイディアが提案されている。しかしながら、ＩＣカードのデータ処理性能は、生体情報を利用する個人認証を行うには著しく不足し、実質的に実現できないものであった。

【０００６】さらに、インターネット上で商取引、選挙が行われる場合など、個人認証とともにインターネットを通じて信用情報がやり取りされる。この場合には信用情報を暗号化することにより、セキュリティを高めているが、送られてきた信用情報が本当に本人の情報であって、リアルタイムに送られてきたかどうかを判断することは困難であった。

【０００７】

【発明が解決しようとする課題】本発明の第一の目的は、情報の記憶量が磁気カードに比べて格段に大きい携帯電子装置と盗難や模倣が困難な生体情報により個人認証を行うシステムであって、特に、携帯電子装置に格納された生体情報を外部に流出させないことによりセキュリティを高めた個人認証システムを提供することにある。

【０００８】本発明の第二の目的は、生体情報が再構成できないように処理されたデータを用いて、データ処理装置と携帯電子装置で協調して個人認証を行うことにより、悪意のある第三者がデータ処理装置を不法に操作してシステムへ不法にアクセスすることを防止する、セキュリティの高い個人認証システムを提供することにある。

【０００９】さらに、本発明の第三の目的は、外部ネットワークを通じて携帯電子装置から送られた情報が個人認証を受け、かつ、決められた時間以内に送られた情報であることを証明できるセキュリティの高い個人認証システムを提供することにある。

【００１０】

【課題を解決するための手段】本発明の携帯電子装置は、第一の生体情報の特徴量を登録データとして記憶するメモリと、データ処理装置から認証の対象となる第二

の生体情報の特徴量を特徴データとして受信する送受信インタフェースと、登録データと特徴データとを比較照合するプロセッサとを有する。

【００１１】また、本発明の生体情報を用いた個人認証方法では、データ処理装置は、入力された生体情報から特徴量を抽出し、抽出した特徴量を特徴データとして携帯電子装置に送信し、携帯電子装置は、特徴データとメモリに記憶されている生体情報の特徴量である登録データとを照合する。さらに、携帯電子装置は照合処理の一部をデータ処理装置により実行することにより、ハードウエア負荷を軽減する。

【００１２】

【発明の実施の形態】図１に、ＩＣカード等に代表される携帯電子装置の構成を示す。携帯電子装置１０は、携帯電子装置１０全体の制御を行うＣＰＵ１０２と、アプリケーションプログラムやデータを格納するＲＡＭ／ＲＯＭ１０３と、携帯電子装置１０と外部との通信を行うＩ／Ｏ１０１とを備える。ＲＡＭ／ＲＯＭ１０３はＥＥＰＲＯＭ(Electronic Erasable Programmable Read Only Memory)により構成できる。ＥＥＰＲＯＭは、電力なしにデータを維持することができ、またデータの書き換えも可能なものである。ＣＰＵ１０２とＲＡＭ／ＲＯＭ１０３とはアドレスバス１０４で、ＣＰＵ１０１とＲＡＭ／ＲＯＭ１０３とＩ／Ｏ１０１とは制御信号データ信号バス１０５で接続されている。ＣＰＵ１０２は、外部からのＩ／Ｏ信号をＩ／Ｏ１０１経由で受け、ＲＡＭ／ＲＯＭ１０３上のアプリケーションプログラムを実行し、実行結果をＲＡＭ／ＲＯＭ１０３に書き込む、あるいはＩ／Ｏ１０１経由で外部に出力する。

【００１３】携帯電子装置１０は１チップの中にハードウエア（１０１～１０５）及びソフトウエア（ＲＡＭ／ＲＯＭ）を封じ込める、あるいは携帯電子装置に対してユーザが一定の操作を加えるとソフトウエアを消去する機能を設けることにより耐タンパー性を実現した装置である。耐タンパー性装置はユーザによるソフトウエアの改竄を防止する機能を備えることにより、本発明の適用される電子商取引等の分野に使用する携帯電子装置として望ましいものである。

【００１４】図２に、ＩＣカードターミナルやＩＣカードリーダー等に代表されるデータ処理装置２０の構成を示す。データ処理装置２０は、プログラムを実行するＣＰＵ２０１と、実行すべきプログラムやデータが格納されているＲＡＭ２０５と、初期プログラムブート用のＲＯＭ２０２と、携帯電子装置と情報のやり取りを行う携帯電子装置Ｉ／Ｏ２０３と、外部ネットワークと情報のやり取りを行う外部Ｉ／Ｏ２０４と、データ処理装置２０に接続される入力装置（キーボードやピンパッド等）２０８と出力装置（ディスプレイやスピーカー等）２０９を制御するユーザＩ／Ｏ２０６とを有しており、上記各構成要素はバス２０７により接続されている。

【００１５】図３に示すように、データ処理装置２０はＩ／Ｏ信号で携帯電子装置１０と接続される。また、データ処理装置２０は、必要に応じて、インターネット等のネットワークを通じて、外部情報処理装置３０と情報のやり取りを行うことが出来るものである。

【００１６】ここで、ＩＣカード等に代表される携帯電子装置内のＣＰＵやＲＡＭ／ＲＯＭは、ハードウエアをコンパクトに実現するため、また電源供給や放熱による制約から、データ処理装置（ＩＣカードターミナルやＩＣカードリーダー等）内のＣＰＵやＲＡＭ／ＲＯＭに比べて、一般的に性能が劣る。

【００１７】（実施例１）図４に本発明に係る個人認証システムの第１の実施例のフローチャートを示す。本実施例での処理は携帯電子装置１０及びデータ処理装置２０で実行される処理を含む。

【００１８】データ処理装置２０に、指紋や網膜パターンあるいは音声、筆跡等の生体情報が入力装置２０８から入力される（ステップ４０１）。入力された生データの特徴をＣＰＵ２０１で抽出処理し（ステップ４０２）、抽出処理して得た特徴データを携帯電子装置１０に送る。

【００１９】携帯電子装置１０では、登録データが格納されているＲＡＭ／ＲＯＭ１０３から登録データを読み出し（ステップ４０３）、データ処理装置２０から送られてきた特徴データと登録データとをＣＰＵ１０２で比較照合する（ステップ４０４）。照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【００２０】本実施例での処理によれば、携帯電子装置に登録された生体情報（登録データ）を外部（データ処理装置等）に出力することなく、かつ、処理量の大きい生体情報（生データ）の特徴抽出処理をＣＰＵ性能の大きいデータ処理装置で実行するために、安全にかつ高速に個人認証を実現できる。

【００２１】ここで、生体情報として指紋を使用する場合の登録データの携帯電子装置への登録方法について説明する。指紋の登録は図２に示したデータ処理装置で行われる。

【００２２】図９に示したように、指紋を入力する入力装置２０８は、光学装置（例えば、ＣＣＤカメラ等を用いた指紋センサ）９０１と光学装置９０１から取り込まれた画像データをデジタル化するデジタル装置９０２とを有する。デジタル化された画像データ（生データ）はデータ処理装置２０に入力される。ＣＰＵ２０１は、生体情報の照合を容易にするために入力された生データから特徴データを抽出するプログラムを実行する。特徴を抽出する方式は様々提案されており、これにより本発明は制約されない。例えば、南他「指紋照合のための新しいセキュリティシステム開発」（エレクトロニクス昭和

６３年９月号）に記載された方法が使用できる。この方法は、図１０に示すように、生データに対して階調変換（ステップ１００１）、平準化（ステップ１００２）、隆線方向抽出（ステップ１００３）の各処理を順に施す。指紋パターンの一例を図１１に示し、詳細に述べる。

【００２３】階調変換１００１は、生データ１１０１の階調（いわゆる色数）を落とす処理である。例えば２５６色の生データを３２色に階調を落とす。平準化１００２は、指紋データには、その画像の性質上、急激な階調変化は少なく、かつ隣接画素間の相関が強いことから、孤立点の除去を行う処理である。これらの処理を行った画像を格子状領域に区分し、各格子状領域における隆線方向を抽出する。各格子状領域について抽出された隆線方向パターンを特徴データ１１０２とする。

【００２４】通常、得られた特徴データ１１０２の周辺領域は、入力装置の光学的歪みなどでノイズが多く含まれている。また、照合に有用な指紋の特徴位置は隆線変化の多い特徴データの中心領域である。そこで、特徴データの特徴位置が多く含まれる中心領域を切り出し、切り出された部分特徴データ１１０３は携帯電子装置１０に送る。携帯電子装置１０は、部分特徴データ１１０３を登録データとしてＲＡＭ／ＲＯＭ１０３に格納する。

【００２５】（実施例２）図５に、本発明に係る個人認証システムの第２の実施例のフローチャートを示す。本実施例では、第１の実施例における携帯電子装置の処理の一部をデータ処理装置で行うことにより、携帯電子装置上の処理の負荷を軽減する。

【００２６】データ処理装置２０に生体情報が入力装置２０８から入力され（ステップ５０１）、入力された生データの特徴をＣＰＵ２０１で抽出処理し、特徴データを得る（ステップ５０２）。携帯電子装置１０は、ＲＡＭ／ＲＯＭ１０３から格納されている登録データを読み出し（ステップ５０５）、読み出した登録データの一部分を切り出し（ステップ５０６）、切り出した部分登録データをデータ処理装置２０に送る。

【００２７】データ処理装置２０では、特徴データと携帯電子装置より送られた部分登録データとから切り出し制御信号を生成し（ステップ５０３）、特徴データを切り出し（ステップ５０４）、携帯電子装置１０に送る。携帯電子装置１０では、切り出された特徴データと登録データとをＣＰＵ１０２で比較照合し（ステップ５０７）、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【００２８】第２の実施例における認証処理をより詳細に説明する。予め登録されている登録データと認証の対象として入力された生体情報の特徴データとを照合するためには、（ａ）登録データと特徴データの正規化処理（指紋を生体情報とする場合には位置合わせ等の処理）と（ｂ）登録データと特徴データの比較処理、の２つの処理が必要である。第２の実施例では正規化処理はデータ処理装置２０で行い、比較処理は携帯電子装置１０で行う。携帯電子装置１０では登録データから正規化処理に必要最低限の部分登録データを抽出する。そして、正規化済み（位置合わせ済み）の特徴データを携帯電子装置１０に送り、携帯電子装置１０で比較処理を行う。これにより、悪意の第三者が携帯電子装置より出力された部分登録データを入手し、別の携帯電子装置にその部分登録データを登録しても、個人認証はできない。

【００２９】図１２に示す指紋データを例に取り、第２の実施例における比較処理の流れを詳細に説明する。認証の対象となる指紋の画像データ１２０４が、入力装置２０８からデータ処理装置２０に入力され、特徴抽出処理が実行されることにより特徴データ１２０５を得る。

【００３０】一方、携帯電子装置１０では、登録データ１２０１を読み出し、位置合わせ用の部分登録データ１２０２を作成する。図１２には、部分登録データ１２０２として登録データ１２０１の四隅を切り出す例を示している。位置合わせ用部分登録データ１３０２は登録データの盗用につながらない限り任意でよい。したがって、指紋の特徴情報を多く含まない登録データの周縁部を切り出すことが望ましく、また、照合するデータの回転を考慮して複数箇所を切り出すことが望ましい。

【００３１】切り出した部分登録データ１２０２はデータ処理装置２０に送られる。データ処理装置２０は、特徴データ１２０５と送られてきた部分登録データ１２０２とから切り出し制御信号を生成する。切り出し制御信号とは、登録データ１２０３に一致する特徴データ１２０５の部分を指示する信号であり、例えば登録データ１３０１の四隅に対応する座標で表される。データ処理装置２０は切り出し制御信号にしたがって特徴データ１２０５に切り出し処理を行う。これにより、４つの箇所からなる位置合わせ用データ１２０２を四隅とする矩形（切り出された特徴データ１２０６）が切り出される。

【００３２】切り出された特徴データ１２０６は、携帯電子装置１０に送られ、登録データ１２０３と比較照合される。

【００３３】第２の実施例では、携帯電子装置に格納された生体情報の登録データを携帯電子装置の外に出力することなく、また、処理量の大きい正規化処理をＣＰＵ性能の大きいデータ処理装置により実行するために、安全、かつ高速な個人認証が実現できる。

【００３４】（実施例３）図６に、本発明に係る個人認証システムの第３の実施例のフローチャートを示す。

【００３５】データ処理装置２０に生体情報が入力装置２０８から入力され（ステップ６０１）、入力された生データの特徴をＣＰＵ２０１で抽出処理し、特徴データを得る（ステップ６０２）。携帯電子装置１０は、ＲＡＭ／ＲＯＭ１０３から格納されている登録データを読み

出し（ステップ６０６）、読み出した登録データの一部分を切り出し（ステップ６０７）、切り出した部分登録データをデータ処理装置２０に送る。

【００３６】データ処理装置２０では、特徴データと携帯電子装置より送られた部分登録データとから切り出し制御信号を生成し（ステップ６０３）、特徴データを切り出す（ステップ６０４）。切り出された特徴データに見込み処理を行い（ステップ６０５）、切り出された特徴データ及び見込み処理データを携帯電子装置１０に送る。携帯電子装置１０では、切り出された特徴データ、見込み処理データ、登録データとをＣＰＵ１０２で比較照合し（ステップ６０８）、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【００３７】生体情報として指紋を使用する場合を例として第３の実施例をより詳細に説明する。

【００３８】照合処理には（ａ）正規化処理、（ｂ）比較処理の２つの処理が含まれることは第２の実施例で説明したとおりである。本実施例ではさらに、比較処理における携帯電子装置の処理負担を軽減する。登録データと特徴データの比較は、両者の距離を計算し、距離の大小から判定するのが一般的である。ここで、距離の関数によっては演算量が多くなり、ハードウエア性能が貧弱な携帯電子装置にとって処理負荷が大きくなる場合がある。

【００３９】本実施例では、もし認証されるべき入力データが本人のものである場合には入力データは登録データの近傍に位置するという点に着目し、切り出された特徴データを近傍の範囲内でずらし、見込み距離を計算する。

【００４０】図１３に具体例を示す。単純化のため、特徴データを構成する隆線方向パターンはｘ軸との角度をａ°とする単位ベクトルで表示されるものとし、特徴データをａで代表させる。ここで、切り出された特徴データ１３０１が、（４１、３３、１８、３７、２２、５、２４、１２、３）であったとする。

【００４１】データ処理装置２０は、例えば、最初の特徴データ「４１」について、その近傍として「－２、－１、０、＋１、＋２」をとり、その絶対値「２、１、０、１、２」を求める。各特徴データについて許容できる近傍の範囲について予め計算した結果が見込み処理データ１３０２である。

【００４２】携帯電子装置１０では、見込み処理データ１３０２を受け、最初の特徴データ「４１」とこれに対応した近傍データ「２、１、０、１、２」を基に、仮に登録データ列が、（４０、３５、２０、３７、２０、８、２８、１０、５）の場合、最初の登録データが「４０」なので、特徴データ「４１」と比較し、差が「－１」なので、見込み処理データ「２、１、０、１、２」から「１」を得る。同様に、次々との登録データと切り出された特徴データとを比較し、対応した見込み処理データから距離を得て、累積加算する。累積加算した結果が、登録データと切り出された特徴データとの差となり、この値が、ある閾値より小さければ、登録データと切り出された特徴データとが一致していると判断する。

【００４３】以上のように、携帯電子装置１０では、計算量の必要な距離計算を行わず、データ処理装置２０で演算を行い、登録データと切り出された特徴データとを比較することにより、見込み処理データからテーブルルックアップ的に距離を得て、照合処理を行う。

【００４４】なお、ここでは、１次元の特徴データを例に説明したが、次元数が増えた場合、また、距離の関数にどのようなものを用いても、携帯電子装置１０の演算負荷を軽くすることができる。

【００４５】（実施例４）図７に、本発明に係る個人認証システムの第４の実施例のフローチャートを示す。

【００４６】データ処理装置２０に生体情報が入力装置２０８から入力され、入力された生データの特徴をＣＰＵ２０１で抽出処理し、特徴データを得る。携帯電子装置１０は、ＲＡＭ／ＲＯＭ１０３から格納されている登録データを読み出す。データ処理装置でのステップ７０１～７０４の処理、携帯電子装置でのステップ７０６、７０７の処理は実施例２、３と同様である。本実施例では、登録データと送られてきた特徴データとの差分を計算する（ステップ７０９）。この差分データに対して、ステップ７０８で発生させた乱数により暗号化処理を行い（ステップ７１０）、暗号化データをデータ処理装置２０に送る。

【００４７】データ処理装置２０では、特徴データと送られた暗号化データで前照合処理を行い（ステップ７０５）、前照合データを携帯電子装置１０に送る。携帯電子装置１０では、前照合データと発生した乱数から後照合処理を行い（ステップ７１１）、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。

【００４８】生体情報として指紋を使用する場合を例として第４の実施例をより詳細に説明する。

【００４９】本実施例も第３の実施例と同様に、比較処理における携帯電子装置の処理負担を軽減することを目的とするものである。本実施例も距離を求める演算をデータ処理装置で行い、その演算結果を携帯電子装置で受け、最終照合処理を行う。

【００５０】携帯電子装置１０では、図１４に示すように、特徴抽出された特徴データ１４０１と登録データ１４０２の差データ１４０３を求める。完全に特徴データの隆線方向ベクトルと登録データの隆線方向ベクトルとが一致すれば結果はゼロベクトルになるが、一般に特徴データには誤差が多く含まれるのでゼロにはならない。

ここで、この差データ１４０３をそのままデータ処理装置に送ると、登録データ１４０２が逆算されてしまう。そこで、差データ１４０３を乱数を使用してスクランブル（データの順序をランダムに並びかえる）し、暗号化データ１４０４としてデータ処理装置に送る。これにより、登録データの逆算を防止できる。

【００５１】データ処理装置２０では携帯電子装置１０で生成された暗号化されたデータの絶対値（角度の差の絶対値を距離とする）を求め、携帯電子装置１０に送る。携帯電子装置１０では距離計算結果を受け、累積加算する。累積加算結果が登録データと切り出された特徴データとの差となり、この値を閾値と比較し（後照合）、閾値より小さければ、登録データと切り出された特徴データとが一致すると判断する。

【００５２】単純化のため、データとして１次元の角度を使用する例で説明したが、２次元データ（例えば、ベクトル終点の座標）等多次元データを使用することももちろん可能である。また、差データを乱数でスクランブルする場合、スクランブルした結果が登録データと同じ次元であると、データ処理装置２０からゼロベクトルや単位ベクトルを繰り返し送ることで、登録データが推論されるおそれがある。そこで、スクランブルにあたっては、暗号化されたデータに乱数で次元数を増やすことにより、推論を困難にすることができる。

【００５３】また、本実施例では正規化処理をデータ処理装置にて行っているが、携帯電子装置のハードウエア性能によっては特徴データをそのまま携帯電子装置に送信し、正規化処理及び差分処理を行わせることも可能である。

【００５４】（実施例５）図８に、本発明に係る個人認証システムの第５の実施例のフローチャートを示す。本実施例は、データ処理装置が外部ネットワークと接続された環境においてセキュリティの高い個人認証システムを実現する。本実施例では、データ処理装置２０はインターネット等のネットワークに接続され、ネットワークにはコンピュータ等の外部情報処理装置３０（例えば、サービス提供者のホストコンピュータ）が接続されている。

【００５５】データ処理装置２０に生体情報が入力装置２０８から入力され（ステップ８０１）、入力された生データの特徴をＣＰＵ２０１で抽出処理し、特徴データを得（ステップ８０２）、携帯電子装置１０に送る。携帯電子装置１０は、ＲＡＭ／ＲＯＭ１０３から格納されている登録データを読み出し（ステップ８０４）、登録データと送られてきた特徴データと照合し（ステップ８０５）、照合結果が真であれば個人認証を正常に終了し、引き続き次の処理を行う。照合結果が偽であれば、個人認証を拒絶し、次の処理を実行しない。以上の照合処理には、上述した第１乃至第４の実施例が適用できる。

【００５６】ここで、データ処理装置２０にユーザにより電子商取引に於ける金銭や取引要求等の情報が入力される。データ処理装置２０は、入力された情報を読み出し（ステップ８０３）、携帯電子装置１０に送る。ユーザによるデータ処理装置への情報の入力もしくは携帯電子装置での個人認証の完了をトリガーとして、外部情報処理装置３０は現在時刻を読み出し（ステップ８０８）、暗号処理（ステップ８０９）を施し、ネットワーク経由で携帯電子装置１０に送る。携帯電子装置１０では、送られてきた暗号化された時刻を解読し（ステップ８０７）、所望の情報と送られてきた時刻とに暗号化処理を施し（ステップ８０６）、データ処理装置２０を通り、ネットワーク経由で外部情報処理装置３０に送る。外部情報処理装置３０では、暗号を解読し（ステップ８１０）、送られてきた時刻が、自分自身が送信した時刻と一致していれば（ステップ８１１）、送られてきた情報が正しい情報であると判断して、所望の情報処理、例えば、電子商取引を行う（ステップ８１２）。

【００５７】本実施例の個人認証システムは、外部情報処理装置３０の指示を受け、データ処理装置からの情報を外部情報処理装置３０に転送する場合に、転送処理を行う者が携帯電子装置１０に登録された者（本人）であることを、外部情報処理装置３０が認識するシステムである。すなわち、本発明による個人認証により第三者が携帯電子装置を悪用して登録された者に成りすますことを防ぎ、かつ、外部情報処理装置３０から送られる時刻を携帯電子装置１０が情報に付加して送り返すことで、データ処理装置２０による改竄を防止する。

【００５８】これにより、携帯電子装置１０に登録された者（本人）がその時刻においてネットワークの向こうに存在していることを証明することができる。このような特性を利用すれば、一定の時間内に処理を行うことを要求されるネットワーク上での競り、選挙に有効なシステムを提供することが可能になる。

【００５９】なお、データ処理装置から必要な情報が送られる例について説明したが、携帯電子装置に登録されている情報、既にデータ処理装置に格納されている情報であっても同様の処理が行える。また、外部情報処理装置において現在時刻の読み出し（ステップ８０８）を行うタイミングがシステムが任意に定めることができる。さらに、外部情報処理装置から現在時刻を携帯電子装置に送信するようにしているが、特に一定の時間内に処理を行うことが要求されていない場合には、時刻に代えて、乱数を送るようにしても同様の効果が達成できる。

【００６０】以上、実施例１から５について詳細に説明した。本発明で使用できる生体情報を指紋を例として説明してきたが、勿論、指紋以外でも、２次元平面に展開できる生体情報、例えば、網膜パターンや手相、人相等、更に筆跡や声紋等のベクトル表現可能なデータ等でも入力処理を変え、特徴抽出のアルゴリズムを変えるだ

けで本発明を実施できる。生体情報を音声とする場合の認証（話者照合）方法について図１５から図１８により説明する。

【００６１】図１５に話者照合のフローチャートを示す。音声を入力し（ステップ１５０１）、入力された音声を音韻に変える（音韻処理、ステップ１５０２）。音韻は音声の特徴量であって、音声のスペクトル解析を基にする。このスペクトル解析による音韻処理としては、中川聖一「確率モデルによる音声認識」第１０頁～第１２頁（電子情報通信学会発行）に記載のＬＰＣケプストラム分析を使用することができる。この音韻処理１５０２の後、音韻処理した音声に対してベクトル量子化処理を行う（ステップ１５０３）。音声の特徴量をベクトル量子化することにより、効率的な計算ができるようになる。このような処理１５０２及び１５０３が生体情報として音声を用いる場合の特徴抽出処理に相当する。また、携帯電子装置１０にはベクトル量子化された音声の特徴量が登録データとして登録され、データ処理装置２０に入力された音声の特徴データと照合される。図１６に示すように、音声の特徴量は特徴ベクトルの時系列として表され、登録データは（A_1, A_2, ・・・A_n）、入力音声の特徴データは（X_1, X_2, ・・・X_n）とする。

【００６２】照合処理（ステップ１５０４）には、ＤＰ（Dynamic Programming）マッチング法やHMM（Hidden Markov Model）法が用いられる。ＤＰマッチング法による照合処理を、図１７を用いて説明する。音声は時間的に伸縮するため時間的変化を許容する照合が必要となる。ＤＰマッチング法では、A_iとX_jとの累積距離が最小とする組合せ（A_i, X_j）（$1 \leqq i \leqq n$, $1 \leqq j \leqq m$）の時系列を求め、その場合の累積距離と所定の基準とを比較することにより照合する。

【００６３】このようにＤＰマッチング法では、何通りもの組合せの時系列について累積距離を計算する必要があるため、計算量を削減することを目的として組合せを一定の範囲に制限することが行われる。この一定の範囲を整合窓と呼ばれ、図１７の直線１７０３と直線１７０４の間にあるような組合せについてのみ累積距離の計算を行う。

【００６４】まず、（A_1, X_j）（$1 \leqq j \leqq r$）の距離を比較し、距離の小さいM個の組合せ候補を抽出し、次に、このM個の候補に対して次時点での組合せ（A_2, X_j）の距離との累積距離を計算し、候補を絞り込む。このような処理を繰り返す。最終的には、組合せ（A_i, X_j）の時系列の中で累積距離を最小とするもの、例えば（A_1, X_1）（A_1, X_2）（A_2, X_3）（A_3, X_3）（A_4, X_4）・・・（A_n, X_n）が抽出される。このようなＤＰマッチング法の詳細については森健一「パターン認識」（電子情報通信学会発行）第１１７頁から第１１９頁に記載されている。

【００６５】このように、話者照合においても、組合せの時系列についての累積距離の計算の処理負荷が大きく携帯電子端末での処理は困難である。そこで、一般に発声の最初においては特徴データに変動が多い一方、発声の途中からは変動が少なくなることから、最初においては整合窓を大きくする必要があるが、途中からは整合窓を比較的に小さくしておいても照合可能である点に着目する。すなわち、発声の前半の照合処理をデータ処理装置で行い（実施例５の「切り出し処理」に対応するものである）、発声の後半の照合処理を携帯電子装置で行う。前半の照合処理のため、登録データが一部分が携帯電子装置からデータ処理装置に送られるが、それ以外の部分は外部に流出することはない。

【００６６】図１８を用いて具体的に説明する。携帯電子装置は登録データA_i（$1 \leqq i \leqq u$）をデータ処理装置に送り、特徴データと照合する。その照合範囲は矩形１８１０に示された範囲となる。この場合の整合窓は広く、直線１８１１と直線１８１２によって挟まれる範囲である。携帯電子装置には照合範囲１８１０での照合結果が送られ、携帯電子装置では引き続きA_i（$u+1 \leqq i \leqq n$）について照合処理が行われる。携帯電子装置での照合範囲は矩形１８２０に示された範囲となり、照合範囲１８２０の整合窓は直線１８２１と直線１８２２によって挟まれる範囲である。このように、携帯電子装置における照合処理では、データ処理装置における照合処理におけるよりも整合窓を狭くして計算負荷を軽減することができる。

【００６７】さらに、上述した実施例３、４に対応する処理を行い、携帯電子装置において計算量を軽減することができる。実施例３に対応して、特徴データX_jの近傍Y_k（$1 \leqq k \leqq l$）との距離を求めたものを見込み処理データとする。A_iと一致するY_kを選択し、見込み処理として予め算出した（Y_k, X_j）の距離を（A_i, X_j）の距離とすることができる。このようにして累積距離を最小とする組合せ（A_i, X_j）の時系列を得ることができる。

【００６８】また、実施例４に対応して差分処理として、組合せ（A_i, X_j）の差を整合窓を満たす時系列としてとり、それに暗号処理を施して前照合処理として組合せ（A_i, X_j）の距離計算を行うことができる。この場合、後照合処理として得られた累積距離からその値を最小とするものを選び、閾値と照合する。

【００６９】このような特徴ベクトル列のマッチング方法は筆跡の照合にも有効なものである。

【００７０】

【発明の効果】本発明により、携帯電子装置に格納された生体情報を外部に流出させないことによりセキュリティを高めた個人認証システムが実現される。

【図面の簡単な説明】

【図１】携帯電子装置の構成を示す図である。

17

【図２】データ処理装置の構成を示す図である。

【図３】携帯電子装置とデータ処理装置と外部情報処理装置との関係を示す図である。

【図４】本発明に係る個人認証処理の第１の実施例を示す図である。

【図５】本発明に係る個人認証処理の第２の実施例を示す図である。

【図６】本発明に係る個人認証処理の第３の実施例を示す図である。

【図７】本発明に係る個人認証処理の第４の実施例を示す図である。

【図８】本発明に係る個人認証処理の第５の実施例を示す図である。

【図９】生体情報として指紋を用いる場合の入力装置の構成を示す図である。

【図１０】指紋の特徴データを求める方法を示す図である。

【図１１】指紋の登録データを作成する方法を示す図である。

【図１２】位置合わせ用データにより位置合わせを行い、登録データと特徴データとを照合する方法を示す図である。

18

＊【図１３】登録データと特徴データとを照合するための見込み処理を説明する図である。

【図１４】登録データと特徴データから差データを求め、暗号化データを生成する図である。

【図１５】生体情報として音声を用いる場合の、話者照合方法を示す図である。

【図１６】生体情報として音声を用いる場合の、登録データと特徴データとを示す図である。

【図１７】話者照合のためのＤＰマッチング法を示す図である。

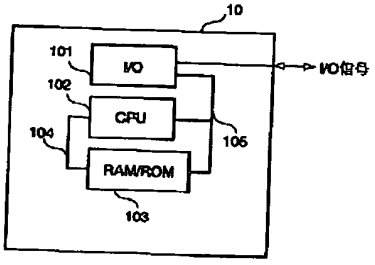
【図１８】本発明における話者照合のためのＤＰマッチング法を示す図である。

【符号の説明】

１０…携帯電子装置、１０１…Ｉ／Ｏ(Input/Output)、１０２…ＣＰＵ(CentralProcessing Unit)、１０３…ＲＡＭ／ＲＯＭ(Random Access Memory/ Read Only Memory)、１０４…アドレスバス、１０５…制御信号・データ信号バス、２０…データ処理装置、２０１…ＣＰＵ、２０２…ＲＯＭ、２０３…携帯電子装置Ｉ／Ｏ、２０４…外部Ｉ／Ｏ、２０５…ＲＡＭ、２０６…ユーザＩ／Ｏ、２０７…バス、２０８…入力装置、２０９…出力装置、３０…外部情報処理装置。

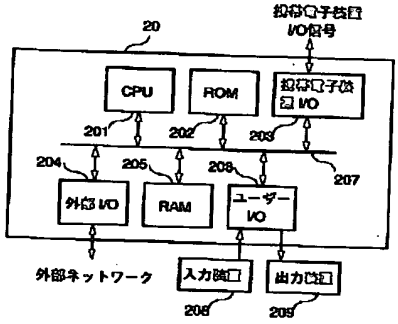
【図１】

図１



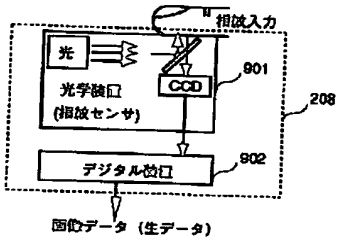
【図２】

図２



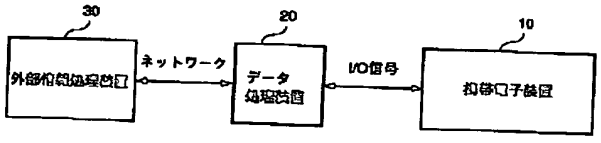
【図９】

図９



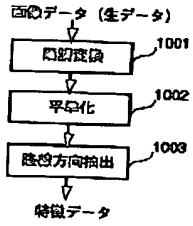
【図３】

図３



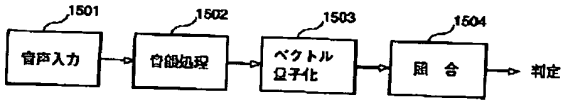
【図１０】

図１０



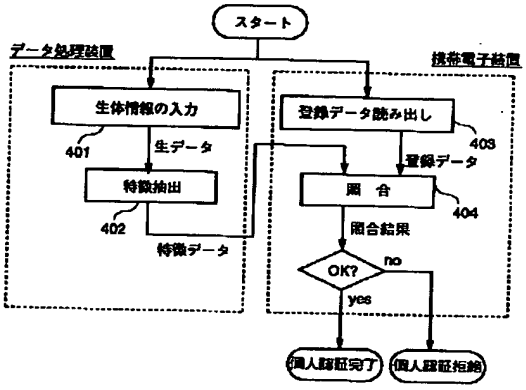
【図１５】

図１５



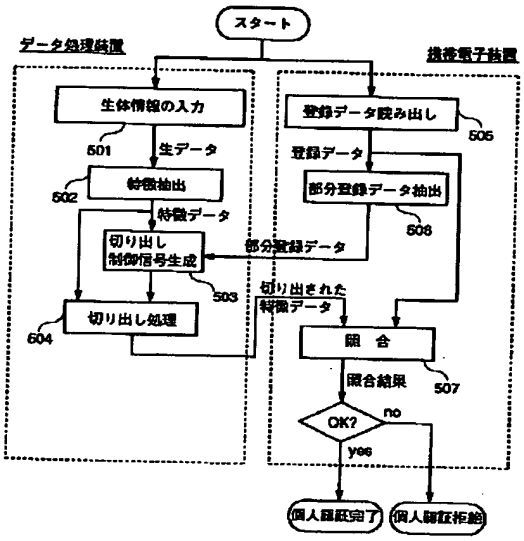
【図４】

図４



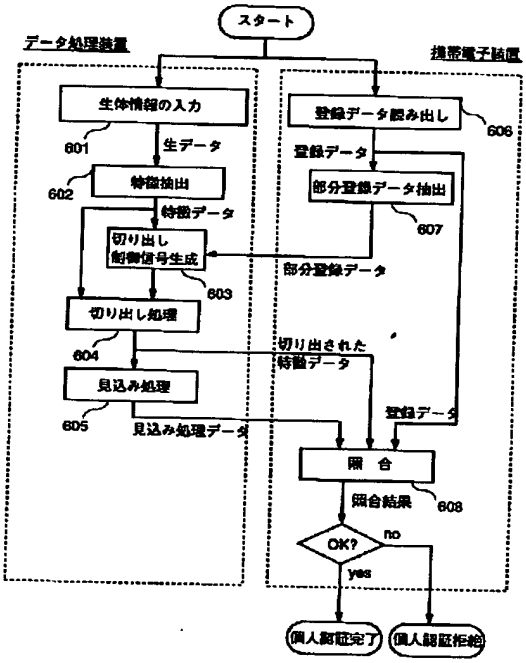
【図５】

図５



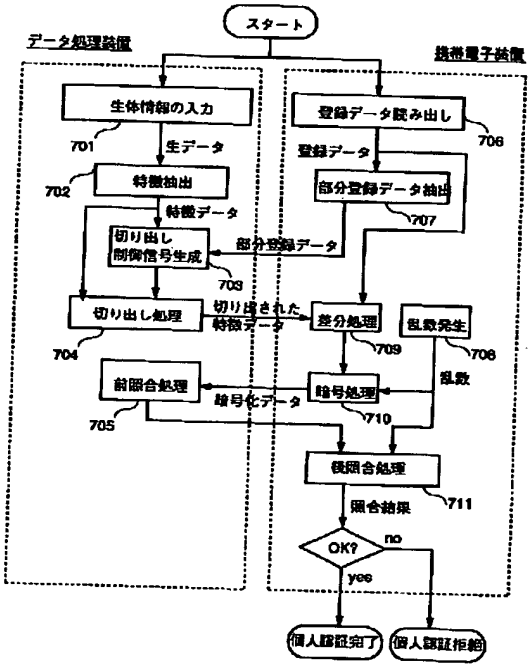
【図６】

図６



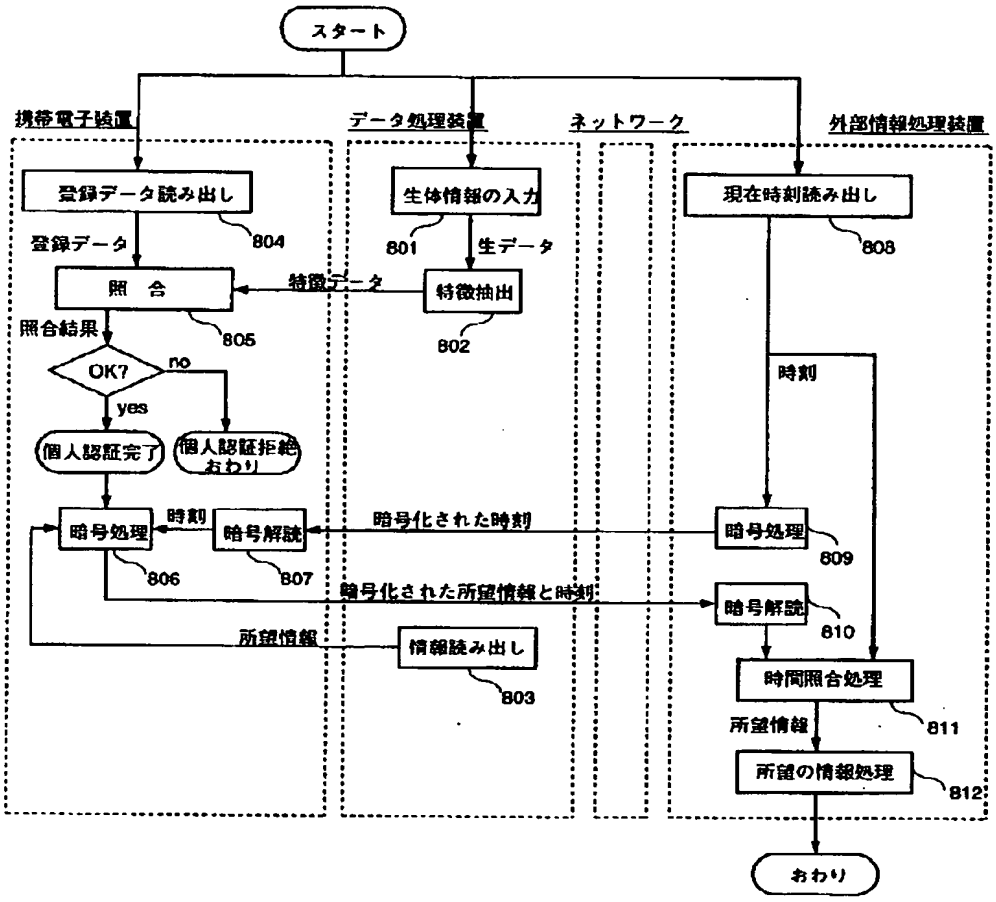
【図７】

図７



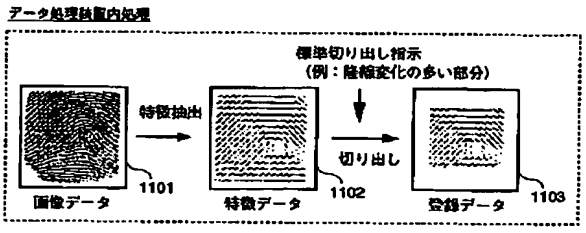
【図８】

図８



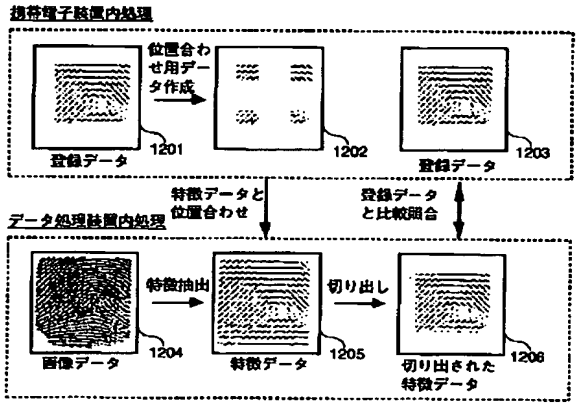
【図１１】

図１１



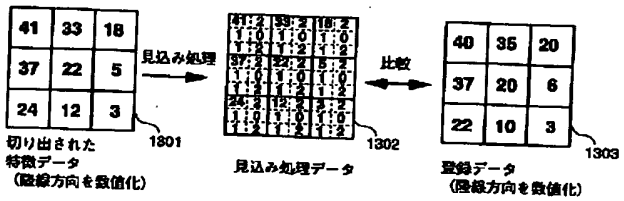
【図１２】

図１２



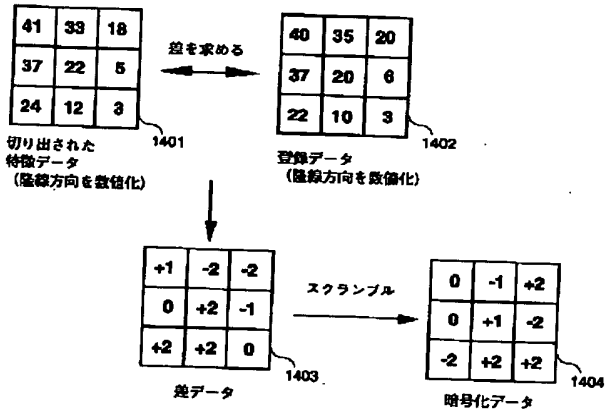
【図１３】

図１３



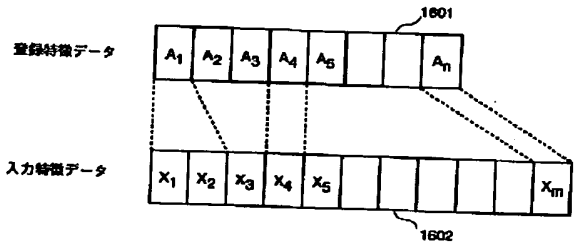
【図１４】

図１４



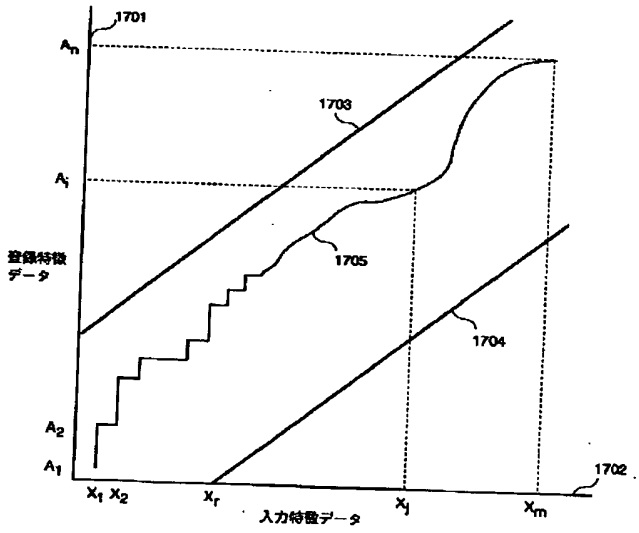
【図１６】

図１６



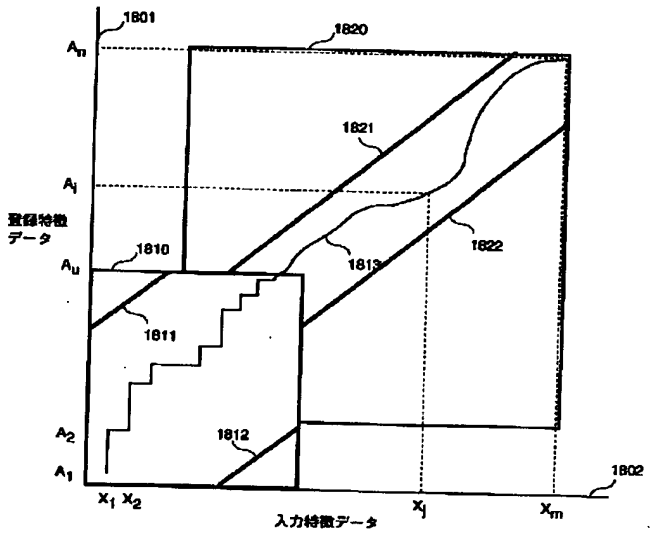
【図１７】

図１７



【図１８】

図１８


1801
1820
A_m
1821
A_j
登録特徴データ
1810
A_u
1813
1822
1811
A_2
1812
A_1
1802
x_1 x_2
x_j
x_m
入力特徴データ